



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/388,195

09/01/1999

EDWARD M. SCHEIDT

STS-127

3506

7590

10/27/2005

IP Strategies PC  
12 1/2 wall Street  
Suite 1  
Asheville, NC 28801

EXAMINER

REVAK, CHRISTOPHER A

ART UNIT

PAPER NUMBER

2131

DATE MAILED: 10/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/388,195

Applicant(s)

SCHEIDT, EDWARD M.

Examiner

Christopher A. Revak

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 15 July 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-60 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-60 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## **DETAILED ACTION**

### ***Response to Arguments***

1. Applicant's arguments with respect to claims 1-60 have been considered but are moot in view of the new grounds of rejection.

### ***Double Patenting***

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

3. Claims 1-60 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-65 of U.S. Patent No. 6,885,747. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1-60 of the instant application are envisioned by patent claims 1-65 in that claims 1-65 of the patent contains all the limitations of claims 1-60 of the instant application. Claims 1-60 of the instant application therefore

are not patentably distinct from the earlier patent claims and as such, is unpatentable for obvious-type double patenting.

4. Claims 1-60 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-67 of U.S. Patent No. 6,542,608. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1-60 of the instant application are envisioned by patent claims 1-67 in that claims 1-67 of the patent contains all the limitations of claims 1-60 of the instant application. Claims 1-60 of the instant application therefore are not patentably distinct from the earlier patent claims and as such, is unpatentable for obvious-type double patenting.

5. Claims 1-60 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-67 of U.S. Patent No. 6,549,623. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1-60 of the instant application are envisioned by patent claims 1-67 in that claims 1-67 of the patent contains all the limitations of claims 1-60 of the instant application. Claims 1-60 of the instant application therefore are not patentably distinct from the earlier patent claims and as such, is unpatentable for obvious-type double patenting.

6. Claims 1-60 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-35 of U.S. Patent No. 6,608,901. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1-60 of the instant application are envisioned

by patent claims 1-35 in that claims 1-35 of the patent contains all the limitations of claims 1-60 of the instant application. Claims 1-60 of the instant application therefore are not patentably distinct from the earlier patent claims and as such, is unpatentable for obvious-type double patenting.

7. Claims 1-60 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-62 of U.S. Patent No. 6,606,386. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1-60 of the instant application are envisioned by patent claims 1-62 in that claims 1-62 of the patent contains all the limitations of claims 1-60 of the instant application. Claims 1-60 of the instant application therefore are not patentably distinct from the earlier patent claims and as such, is unpatentable for obvious-type double patenting.

### ***Claim Rejections - 35 USC § 102***

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 1-6 and 21-26 are rejected under 35 U.S.C. 102(e) as being anticipated by Morgan et al, U.S. Patent 6,185,685.

As per claims 1 and 21, it is disclosed by Morgan et al of a method and storage medium comprising instructions for causing a data processor to encrypt an object. A plurality of key splits are combined to generate a cryptographic key. A cryptographic algorithm is initialized with a cryptographic key and the initialized cryptographic algorithm is applied to the object to form an encrypted object. One of the plurality of key splits corresponds to a part of a biometric measurement (col. 3, line 51 through col. 4, line 23 and col. 14, lines 34-43).

As per claims 2 and 22, it is taught by Morgan et al that for one of the plurality of key splits, at least one key split is added to the encrypted object (col. 3, lines 51-67).

As per claims 3 and 23, Morgan et al discloses that for one of the plurality of key splits, reference data associated with at least one key split is added to the encrypted object (col. 8, lines 34-37).

As per claims 4,5,24, and 25, Morgan et al teaches of retrieving at least one of the plurality of key splits from a storage medium, wherein the storage medium is disposed on a smart card (col. 14, lines 20-40).

As per claims 6 and 26, Morgan et al discloses of combining a plurality of key splits to generate a cryptographic key is performed on a smart card (col. 14, lines 20-40).

10. Claims 1-3,7-23, and 27-60 are rejected under 35 U.S.C. 102(e) as being anticipated by Scheidt et al, U.S. Patent 6,885,747.

As per claims 1 and 21, it is disclosed by Scheidt et al of a method and storage medium comprising instructions for causing a data processor to encrypt an object. A

plurality of key splits are combined to generate a cryptographic key. A cryptographic algorithm is initialized with a cryptographic key and the initialized cryptographic algorithm is applied to the object to form an encrypted object. One of the plurality of key splits corresponds to a part of a biometric measurement (col. 1, lines 9-14 and col. 5, lines 13-26 & 44-50).

As per claims 2 and 22, it is taught by Scheidt et al that for one of the plurality of key splits, at least one key split is added to the encrypted object (col. 1, line 9-14 and col. 2, line 64 through col. 3, line 10).

As per claims 3 and 23, Scheidt et al discloses that for one of the plurality of key splits, reference data associated with at least one key split is added to the encrypted object (col. 2, line 64 through col. 3, line 10).

As per claims 7 and 27, it is taught by Scheidt et al of system and storage medium comprising instructions associated with an organization for causing a data processor to encrypt an object by a user. A cryptographic key is generated by combining an organization split corresponding to an organization, a maintenance split, a random split, and at least one label split. A cryptographic algorithm is initialized with the cryptographic key and the object is encrypted according to the initialized cryptographic algorithm. Combiner data is added to the object wherein the combine data includes reference data corresponding to at least one of the label split and the cryptographic algorithm, name data associated with the organization, at least one of the maintenance split and maintenance level associated with the maintenance split, and the random split

and then storing the encrypted object with the added combiner data (col. 1, lines 9-14, col. 2, line 54 through col. 3, line 10, col. 4, lines 14-23).

As per claims 8 and 28, the teachings of Scheidt et al disclose of selecting at least one label split from at least one credential (col. 2, lines 49-51).

As per claims 9 and 29, it is disclosed by Scheidt et al wherein the selected label split is encrypted, the cryptographic key is a first cryptographic key. A second cryptographic key is derived from a user ID associated with the user, a password associated with the user, and at least one of a unique data instance and a random value and then decrypting the selected label split with the second cryptographic key (col. 2, lines 49-51 col. 3, line 51 through col. 4, line 14, and col. 5, line 60 through col. 6, line 5).

As per claims 10 and 30, Scheidt et al teaches that the credential is retrieved from memory (col. 2, lines 49-51).

As per claims 11 and 31, the disclosure of Scheidt et al recites that the memory is disposed on a smart card (col. 4, lines 13-14).

As per claims 12,14,32, and 34, Scheidt et al discloses of generating a time stamp corresponding to a time at which the object was encrypted, wherein the combiner data includes the time stamp (col. 4, lines 39-46).

As per claims 13 and 33, the teachings of Scheidt et al disclose that the combiner data includes a user ID associated with the user (col. 2, lines 23-29 & 49-51).

As per claims 15 and 35, Scheidt et al teaches that the combiner data is a header record (col. 2, lines 23-29).



As per claims 16,17,36, and 37, it is disclosed by Scheidt et al that the combiner data includes a digital certificate and a digital signature (see abstract and col. 5, lines 18-23).

As per claims 18 and 38, Scheidt et al teaches that the cryptographic key is a first cryptographic key and a second cryptographic key is generated based on a label split, the random split is encrypted with the second cryptographic key, prior to adding the combiner data to the encrypted object, and the random split included in the combiner data is the encrypted random split (col. 1, lines 9-14, col. 2, line 64 through col. 3, line 10, and col. 4, lines 14-23).

As per claims 19 and 39, Scheidt et al discloses that before adding the combiner data to the encrypted object, a portion of the combiner data is encrypted with a header split (see abstract).

As per claims 20 and 40, Scheidt et al teaches that the header split is constant (see abstract).

As per claims 41,46,51, and 56, it is disclosed by Scheidt et al of combining the organization split, the maintenance split, the random split, and the label split includes applying a non-linear function to the splits (col. 2, lines 40-54 and col. 3, lines 14-15).

As per claims 42,47,52, and 57, Scheidt et al teaches that the cryptographic key is a single-integer cryptographic key (col. 3, lines 14-15).

As per claims 43,48,53, and 58, it is taught by Scheidt et al that the organization split, the maintenance split, the random split, and the label split are provided by a policy manager and a credentials manager (col. 2, lines 40-54).

As per claims 44,49,54, and 59, Scheidt et al discloses that the cryptographic algorithm is a symmetrical algorithm (col. 3, lines 14-15).

As per claims 45,50,55, and 60, it is taught by Scheidt et al that the cryptographic key is a session key (col. 3, lines 14-15).

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-3:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
CR

October 23, 2005

Christopher Revak  
Primary Examiner

AU 2131



10/23/05